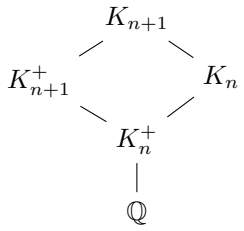
# Week 8: Field extensions and geometry (14.4, 14.5)

## Practice Problems

1. Find a Galois extension $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong C_3$.
2. Without appealing to the fundamental theorem of algebra, show that every polynomial in $\mathbb{R}[x]$ of odd degree has a root in $\mathbb{R}$. Deduce that there are no nontrivial odd-degree extensions of $\mathbb{R}$.
3. Without appealing to the fundamental theorem of algebra, show that every polynomial in $\mathbb{C}[x]$ of degree 2 has a root in $\mathbb{C}$. Deduce that there are no quadratic extensions of $\mathbb{C}$.

## Presentation Problems

1. Let $p$ be an odd prime and let $\zeta_p = e^{2\pi i/p}$. Show that there exists a unique quadratic extension $K/\mathbb{Q}$ with $K \subseteq \mathbb{Q}(\zeta_p)$. What is this quadratic extension?
2. Show that $\sqrt[3]{2}$ is not contained in any cyclotomic field over $\mathbb{Q}$.
3. For each integer $n \geq 1$, set $K_n = \mathbb{Q}(\zeta_{2^{n+2}})$ and $K_n^+ = \mathbb{Q}(\alpha_n)$ where $\alpha_n = \zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}$.
   (a) Show that $K_n^+ = K_n \cap K_{n+1}^+$ and determine the degrees of the extensions in the diagram




   (b) Determine the minimal polynomials for $\zeta_{2^{n+2}}$ and $\alpha_{n+1}$ over $K_n^+$, with coefficients in terms of $\alpha_n$.
   (c) Inductively give an explict formula for $\alpha_n$ using nested square roots.
4. For each $n \geq 1$, determine $\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n)$ and $\mathrm{N}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n)$. Your answer will depend on the prime factorization of $n$.

## Group Theory Problem

1. (a) Let $1 \to A \to E \to G \to 1$ be a short exact sequence of groups. Show that if $A$ is abelian then the conjugation action gives a well-defined $G$-module structure on $A$.

   Let $G$ be a finite group and let $A$ be a $G$-module. A group extension of $G$ by $A$ is a short exact sequence of groups $1 \to A \to E \to G \to 1$ such that original $G$-module structure on $A$ agrees with the conjugation $G$-module structure on $A$. Two extensions $1 \to A \to E \to G \to 1$ and $1 \to A \to E' \to G \to 1$ of $G$ by $A$ are said to be equivalent if there is a group homomorphism $f\colon E \to E'$ making the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_A} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}_G} & & \\ 1 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

   commute.

   (b) Show that equivalence of group extensions is an equivalence relation.

Recall the definitions of $Z^2(G,A)$ and $B^n(G,A)$ from last week.

(c) Show that

$$Z^2(G,A) = \{f\colon G\times G\to A\colon f(g,h)+f(gh,k) = gf(h,k)+f(g,hk) \text{ for all } g,h,k\in G\},$$
$$B^2(G,A) = \{(g,h)\mapsto gf(h)-f(gh)+f(g) \text{ for all } g,h\in G\colon f\colon G\to A\}.$$

Let

$$1 \longrightarrow A \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$$

be an extension of $G$ by $A$. A section of $\pi$ is a set-function $\mu\colon G\to E$ such that $\pi\circ\mu = \mathrm{id}_G$.

(d) Show that sections of $\pi$ exist.

(e) Let $\mu\colon G\to E$ be a section of $\pi$. Show that there exists a unique function $f_\mu\colon G\times G\to A$ such that $\mu(g)\mu(h) = f_\mu(g,h)\mu(gh)$ for all $g,h\in G$.

(f) Show that this construction gives a well-defined map from equivalence classes of extensions of $G$ by $A$ to elements of the quotient group $Z^2(G,A)/B^2(G,A)$.

(g) Construct an inverse map in the opposite direction by defining a group structure on $A\times G$ by

$$(a_1,g_1)\cdot(a_2,g_2) = (a_1+g_1a_2+f(g_1,g_2),g_1g_2)$$

for any $f\in Z^2(G,A)$.

(h) Show that equivalence classes of extensions of $G$ by $A$ are in bijection with elements of $H^2(G,A)$.

## Tricky Problems

1. (a) For each $n\geq 1$, compute the lattice of subfields for the extension $\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}$.
   (b) Compute $\mathrm{Gal}(K/\mathbb{Q})$ for each intermediate field $K$ of the extension $\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}$.

2. Let $f(x)\in\mathbb{C}[x]$ and let $g(x) = f(x)\overline{f}(x)$ where $\overline{f}(x)$ is given by taking the complex conjugate of the coefficients of $f$.

   (a) Show that $g(x)\in\mathbb{R}[x]$.

   Let $K$ be the splitting field of $g(x)$ over $\mathbb{R}$.

   (b) Show that $K(i)$ is a Galois extension of $\mathbb{R}$.

   Let $G = \mathrm{Gal}(K(i)/\mathbb{R})$ and let $P$ be a Sylow 2-subgroup of $G$.

   (c) Show that the fixed field of $P$ is an extension of $\mathbb{R}$ of odd degree. Deduce that $G$ is a 2-group.

   (d) Show that if $\mathrm{Gal}(K(i)/\mathbb{C})\neq 1$ then there exists a quadratic extension of $\mathbb{C}$. Deduce that $K(i) = \mathbb{C}$.

   (e) Show that if $g(x)$ is nonconstant then $g(x)$ has a root in $\mathbb{C}$.

   (f) Show that if $f(x)$ is nonconstant then $f(x)$ has a root in $\mathbb{C}$.

   This is known as the fundamental theorem of algebra.